REMARKS

Reconsideration and allowance of the subject application are respectfully requested.

Claims 1-7 were pending prior to the Office Action of September 12, 2003. Claims 1 and 4 are currently amended herein. Support for the amendments to claims 1 and 4 can be found throughout the specification, more specifically, on page 20, lines 24-26, page 21, lines 4-6, and page 30, lines 22-24. Accordingly, claims 1-7 are still pending in the present application.

The Office Action indicates the information disclosure statement filed on December 21, 1999 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each U.S. and foreign patent; each publication of that portion of which caused it to be listed; and all other information or that portion which caused it to be listed. The Examiner has asserted that several foreign patent documents and a non-patent document or not submitted and thus have not been considered by the office. The Examiner then referenced the IDS on paper No. 9. However, the IDS on paper No. 9 was filed on September 27, 2002 and was returned by the Examiner with only some of the references being acknowledged. In response, Applicant filed a Request for Acknowledgment of Information Disclosure Statement on September 25, 2003.

Furthermore, in hopes of resolving this matter quickly and efficiently, Applicant encloses herein copies of the references cited in the IDS on paper No. 9 as instructed by the Examiner in the Office Action. Thus, Applicant respectfully requests that the Examiner acknowledge the remaining references in the IDS on paper No. 9 and send to Applicant a written copy of such acknowledgment.

The Examiner has also objected to the title for being non-descriptive. In response, Applicant has amended the title herein to be more descriptive as suggested by the Examiner. Thus, Applicant respectfully requests that the objection to the title be withdrawn.

Furthermore, the Examiner has objected to the specification because of numerous grammatical informalities as follows: on page 6, line 9, the phrase "the schemes themselves do not help specifying who is the key holder" should read "the schemes themselves do not specify who is the key holder"; on page 6, line 14, the phrase "one very appearing feature"

should read "one very appealing feature"; on page 6, line 22, the sentence is not grammatical; on page 7, line 2, the sentence is not grammatical; on page 9, line 5, the indefinite article 'an' should be 'a'; on page 20, line 16, there is an extraneous indefinite article; on page 23, line 5, the sentence is not grammatical; on page 43, line 21-22, the sentence is not grammatical. In response, Applicant has amended the specification herein as suggested by the Examiner. Thus, withdrawal of the objections to the specification is hereby respectfully requested.

The Examiner has rejected claims 1-4 under 35 U.S.C. § 102(b) as being anticipated by Schneier's Applied Cryptography.

With respect to claim 1, the Examiner asserts that Schneier teaches a method for protecting a data file on a computer system by encrypting the data file using a key to create an encrypted data file, generating a new key, updating the encrypted data file with the new key to create an updated encrypted data file and replacing the encrypted data file with the updated encrypted data file, and replacing the key with the new key. The Examiner also asserts that Schneier teaches that keys must be replaced regularly and that old keys must be destroyed. Additionally, the Examiner asserts that Schneier teaches a focal point of encryption such that encryption makes files unrecoverable without the key.

In response, Applicant has currently amended independent claims 1 and 4. Currently amended claim 1 recites a method for protecting a data file on a computer system, comprising the steps of encrypting the data file using a private key to create an encrypted data file, generating a new key, generating a transformation key from the old key and the new key, updating the encrypted data file with the transformation key to create an updated encrypted data file, replacing the encrypted data file with the updated encrypted data file, and replacing the private key with the new key, wherein the updating of the encrypted data file with the transformation key does not reveal the data file during the process of updating.

Thus, according to amended claim 1, after the data file is encrypted and a new key is generated, a transformation key is generated based on the old key and the new key. The encrypted data file is then updated with the transformation key to create an updated encryption data file, while not revealing the data file. Thus, during the process of claim 1, the data file is not revealed during the process of updating. Accordingly, because of the updating

of the encrypted data file with the transformation key, if the original key becomes compromised, the encryption remains secure because of the further transformation. Thus, amended claim 1 eliminates the threat of a compromised key.

Schneier does not suggest this unique double encryption and transformation which renders the original key obsolete upon the transformation of the encrypted data file by the transformation key. Instead, Schneier teaches to re-encrypt data with an encryption key, and that the encryption keys should expire periodically like passports and licenses. (Schneier, page 183) Similarly, Schneier teaches that, depending on the value of the data and the amount of data encrypted during a given period, keys could be replaced as frequently as once a day, assuming there is an efficient method of transferring new keys. (Schneier, page 184) Inherent in a decryption and a re-encryption is the possibility of exposure of the original data file. This exposure is prevented by amended claim 1 by providing a transformation key which updates the encrypted data file, as encrypted by the old key, into an updated encrypted data file equivalent to an encrypted data file encrypted with the new key, without decrypting the encrypted data file during the encryption cycle.

Schneier does not teach to utilize a double encryption and transformation wherein the first encryption key is used as a basis for a transformation key which further transforms the encrypted data file, as is taught by amended claim 1. Thus, Applicant asserts that amended claim 1 is in condition for allowance, and respectfully respects that the rejection of claim 1 under 35 U.S.C. § 102(b) as being anticipated by Schneier's Applied Cryptography be withdrawn.

The Examiner has also rejected claims 2 and 3 in light of Schneier. With respect to claim 2, the Examiner asserts that Schneier teaches a method for protecting a data file on a computer system wherein keys must be replaced regularly, thereby teaching to repeat the updating step and the two replacement steps on a periodic basis. With respect to claim 3, the Examiner asserts that Schneier teaches a method for protecting a data file on a computer system wherein the encryption key is replaced, which is operatively identical to replacing the encryption key for those systems utilizing symmetric keys.

By virtue of their dependency on amended claim 1, which is currently in condition for allowance, claims 2 and 3 are also in condition for immediate allowance. Thus, Applicant respectfully requests that the rejection of claims 2 and 3 under 35 U.S.C. § 102(b) as being anticipated by Schneier's Applied Cryptography be withdrawn.

With respect to claim 4, the Examiner asserts that claim 4 is an apparatus claim corresponding to claims 1-3 and thus does not teach above the information claimed in claims 1-3. As such, the Examiner rejects claim 4 for the same reasons set forth above in the rejections of claims 1-3. In response, Applicant has amended claim 4 in the same manner as amended claim 1. Thus, amended claim 4 recites a processor-driven system adapted to protect a data file, the system comprising a processor, and a memory coupled to the processor for storing the data file, wherein the processor is programmed to perform the steps of encrypting the data file using a private key to create an encrypted data file, generating a new key, generating a transformation key from the old key and the new key, updating the encrypted data file with the transformation key to create an updated encrypted data file, replacing the encrypted data file with the updated encrypted data file, and replacing the private key with the new key, wherein the updating of the encrypted data file with the transformation key does not reveal the data file during the process of updating.

Amended claim 4 is patentable over Schneier for the reasons stated above with reference to amended claim 1. Since the rejection of claim 4 was made for the same reasons as claim 1, the argument made for claim 1 above are equally applicable here. Thus, amended claim 4 is in condition for allowance, and Applicant respectfully requests that the rejection of amended claim 4 under 35 U.S.C. § 102(b) as being anticipated by Schneier's Applied Cryptography be withdrawn.

The Examiner has also rejected claims 5-7 as being unpatentable over Schneier in light of U.S. Patent No. 5,761,306 issued to Lewis. In particular, the Examiner asserts that Lewis discloses a smart card that is implemented in a processor-driven system wherein the smart card includes a processor for protecting personal data and a memory coupled to the processor for storing personal data. Additionally, the Examiner asserts that Lewis teaches a key server used to create new keys for the smart card when the existing key stored on the smart card needs to be replaced. Finally, the Examiner asserts that Lewis teaches a

processor-driven system comprising a communication interface. Thus, the Examiner asserts that it would have been obvious for a person of ordinary skill in the art at the time the invention was made to implement a processor and memory with functions as outlined in claim 4 into a smart card as disclosed by Lewis.

However, since claims 5-7 are dependent on amended claim 4, and amended claim 4 is in condition for allowance over Schneier for the reasons stated above, claims 5-7 are also in condition for allowance. Lewis does not teach or suggest the deficiencies of Schneier as stated above. Thus, Applicant respectfully requests that the rejection of claims 5-7 be immediately withdrawn and claims 5-7 be placed in condition for allowance.

In view of the foregoing, it is submitted that the present application is in condition for allowance and a notice to that effect is respectfully requested. However, if the Examiner deems that any issue remains after considering this response, he is invited to call the undersigned to expedite the prosecution and work out any such issue by telephone.

Respectfully submitted,

Marc S. Kaufman
Registration No. 35,212

MSK:SMH

NIXON PEABODY LLP
401 9th Street, NW
Washington, DC 20004
(202) 585-8000